The Claims

1. (Currently amended) In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a software identity register, a method for booting the operating system comprising:

computing a cryptographic function of at least a portion of the operating system; and

setting the software identity register to a result of the computed cryptographic function if ~~the~~ atomic execution of ~~the~~ a boot block of the operating system does not fail, and otherwise setting the software identity register to a value indicating that the atomic execution of the boot block failed.

2. (Original) The method as recited in claim 1, further comprising defining a secure storage space, access to which is based in part on the result set in the software identity register.

3. (Previously presented) In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a software identity register, a method for booting the operating system comprising:

executing an atomic operation to set an identity of the operating system into the software identity register of the CPU, wherein in an event that the atomic operation completes correctly, the software identity register contains the identity of the operating system and in an event that the atomic operation fails to complete

correctly, the software identity register contains a value indicating that the atomic operation failed; and

examining a content of the software identity register to verify the identity of the operating system.

4. (Currently amended) The method as recited in claim 3, wherein the identity comprises a public key of a correctly signed block of code from the operating system, and examining a content of the software identity register comprises verifying a signature of the signed block of code against the public key.

5. (Original) The method as recited in claim 3, wherein the identity comprises a hash digest of a block of code from the operating system, and examining a content of the software identity register comprises hashing the block of code.

6. (Original) The method as recited in claim 3, further comprising appending at least a portion of the identity to a boot log.

7. (Original) The method as recited in claim 3, further comprising authenticating additional blocks of code.

8. (Original) The method as recited in claim 3, further comprising:

appending at least a portion of the identity to a boot log;

authenticating additional blocks of code; and

appending identities of the additional blocks of code to the boot log.

9. (Original) The method as recited in claim 3, further comprising generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the operating system.

10. (Previously presented) The method as recited in claim 9, further comprising encrypting data using the storage key and storing the encrypted data on the computer system.

11. (Previously presented) In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a software identity register, a method comprising:

identifying a boot block of code in the OS that uniquely describes the OS;

creating an identity of the OS from the boot block; and

executing an atomic operation to set the identity of the operating system into the software identity register of the CPU, wherein in an event that the atomic operation completes correctly, the software identity register is set to contain the identity of the operating system, and in an event that the atomic operation does not complete correctly, the software identity register is set to contain a false value to indicate failure of the atomic operation.

12. (Original) The method as recited in claim 11, wherein creating an identity of the OS comprises signing the boot block using a private key from a key pair to form a signature, the signature and a corresponding public key from the key pair forming the OS identity.

13. (Original) The method as recited in claim 11, wherein creating an identity of the OS comprises hashing the boot block to form a digest, the digest forming the OS identity.

14. (Original) The method as recited in claim 11, further comprising appending at least a portion of the identity to a boot log.

15. (Original) The method as recited in claim 11, further comprising authenticating additional blocks of code.

16. (Original) The method as recited in claim 11, further comprising:
appending at least a portion of the identity to a boot log;
authenticating additional blocks of code; and
appending identities of the additional blocks of code to the boot log.

17. (Original) The method as recited in claim 11, further comprising generating a storage key for encrypting data to be stored on the computer system from a seed based in part on the identity of the OS.

18. (Original) The method as recited in claim 17, further comprising encrypting data using the storage key and storing the encrypted data on the computer system.

19. (Previously presented) In a computer system having a central processing unit (CPU) and an operating system (OS), the CPU having a pair of private and public keys and a software identity register that holds an identity of the operating system, a method comprising:

creating an OS certificate including the identity from the software identity register, information describing the operating system, and the CPU public key; and

signing the OS certificate using the CPU private key.

20. (Original) The method as recited in claim 19, further comprising submitting the signed OS certificate over a network to a third party to prove an identity of the operating system to the third party.

21. (Original) The method as recited in claim 19, wherein creating an identity of the OS comprises forming the OS certificate with one or more items from a boot log containing identities of software components that are executing on the CPU.

22-77. (Canceled).